3.2. Design-Related SMA Processes

3.2.1 Material Allowables

The X-34 vehicle is largely a composite material construction. Three composite vendors support the program: 1) Vermont Composites (fuselage), 2) Aurora Flight Sciences (wing), and 3) R-Cubed (control surfaces). NASA Report 4078, "Composite Spacecraft Structural Design Guide" was employed by the X-34 design team.

The traditional "A-basis" allowable criteria requires that 99% of the specimens in a production lot (or from a stable and controlled process) exceed the structural performance A-basis limit. This requirement must be demonstrated through a statistical sampling procedure necessary to achieve a 95% level of confidence. Most aerospace metallic structural components (such as 7000 series aluminum) are well-characterized and A-basis values are available, and can be found in Mil Handbook 5F. In the case of composite material where not as much statistical data is available, "B-basis" criteria are employed. B-basis performance criteria are defined in terms of the performance level that 90% of the specimens will exceed, demonstrated with a 95% level of confidence. The X-34 uses A-basis allowables for all metallic components and B-basis allowables for all composite components.

3.2.2 Design Factors of Safety

Design limit load is the predicted worst case ground, flight, or recovery load including all uncertainties, specifically, variance in thermal, pressure, and flight loads. Design limit is determined by a 3-sigma high case derived from a Monte Carlo simulation of flight trajectories. Design yield load is design limit multiplied by yield factor of safety. Design ultimate load is design limit multiplied by ultimate factor of safety.

Yield (or 1^{st} ply failure for composites) Safety Factor = 1.25
Ultimate Safety Factor = 1.5

Structural acceptance tests are conducted to design limit level. Protoflight testing is conducted to design yield level. These tests are repeated to Limit Levels to insure that the structure has not been damaged.

3.2.3 Computer Aided Design (CAD)

The X-34 program uses the "Ideas Master Series" software for CAD. This design-tool developed by Structural Dynamics Research Corporation, provides full 3D modeling capability used for interference checking, and library storage of parts and assemblies. The system is accessible for all users. The system allows one-user modification of parts and notification of part and assembly changes. Ideas incorporates an integrated finite element stress analysis capability including composite laminate analysis. OSC employs this tool as a design

environment and communication tool with vendors but stops short of the "paperless design" concept. Printed drawings are still used as the "design release" medium for all manufacturing activity. As discussed in other sections of this document, concurrent engineering is implemented in informal meetings as well as formal subsystem reviews.

3.2.4 Failure Modes, Effect & Criticality Analysis (FMECA) Process / FMEA

The conventional purpose of doing a Failure Mode Effects and Criticality Analysis (FMECA) is to assist and support the iteration of hardware and software design activity. After the design is baselined, the purpose of the FMECA and its derivative, the CIL, is to serve as a tool to aid program management in understanding and managing the risks inherent in the design and to document parameters which will assist in manufacturing process control, assembling interfaces, flight system operations, software development, and the test and evaluation of Government-Furnished-Equipment. The FMECA is not generated as a deliverable to the Government program office but is used by Orbital Science Corporation as an information tool to support the decisions made by the design, development, test , and evaluation, and operation teams. The CIL is not generated for this program because the X-34 is a single string design for all areas except the Flight Termination System (FTS). The following table provides a synopsis of the current status of FMECA development on the X-34 program.

Main Propulsion System:	95% complete
Hydraulics	90% complete
Flight Termination System:	70% complete
Avionics	50% complete
Structures :	FMECA performed as part of the design and not formally documented

The FMECA is also employed (along with Hazard Analysis and Fault Tree Analysis) in developing the integrated (ground & flight) safety analyses contained in the ARAR Accident Risk Assessment Report.

3.2.5 Test and Verification

The X-34 design is verified by a series of material qualification tests at the laminate level to verification and proto-flight tests at the assembly level. Quality is assured at all levels of fabrication including certification of fiber properties, lot and batch testing of pre-preg material and witness coupon testing for each laminate cured. Acceptance tests are conducted for all components and assemblies. Figure 3.9 shows a typical design/test and verification process. Each structural element is tracked and indexed by load case and critical failure mode. For each element the verification method (analysis, handbook data, coupon test, element test, protoflight test) is identified along with applicable testing protocol definition. The flow diagram in Figure 3.10 shows the multi-level testing approach employed on the X-34 program for the case of a

composite structural element, beginning at the fiber level and progressing to integrated structure testing.

Figure 3.9 Test and Verification Process

Structure Verification Matrix Example : Wing

Element	Sub-Element	Load Case	Failure Mode	Verification Method						Test Identification
Spar	Upper Cap	Pull-Up, Landing	Compression	A		CT		PT		MQT-1, WST-1,-2
	Lower Cap	Pull-Up, Landing	Tension	A		CT		PT		MQT-2, WST-1,-2
	Web	Pull-Up, Landing	In-Plane Shear	A		CT		PT		MQT-3, WST-1,-2
	Web Core	Pull-Up, Landing	Core Shear, Core Bond	A	HD		ET	PT		HCS-1,-2,-3
	Spar Skin	Pull-Up, Landing	Buckling	A				PT		WST-1,-2
Skin	Upper Skin	Pull-Up	Compression	A		CT		PT		MQT-1,-2,-3, WST-1
		Pull-Up	Buckling	A				PT		WST-1
		Max Torsion	Shear	A		CT		PT		WST-4
		Transonic Max Lift	Normal Pressure	A		CT		PT		MQT-1,-2,-3, WST-1
	Up Skin Core	Pull-Up, Max Lift	Core Shear, Core Bond	A	HD		ET			HCS-1,-2,-3
	Lower Skin	Pull-Up	Tension	A		CT		PT		MQT-1,-2,-3, WST-1
		2.5 psi Venting	Normal Pressure	A		CT		PT		MQT-1,-2,-3, WST-1
	Low Skin Core	Pull-Up, Max Lift	Core Shear, Core Bond	A	HD		ET			HCS-1,-2,-3
	Main Gear Door	2.5 psi Venting	Normal Pressure	A		CT		PT		MQT-1,-2,-3, WST-1
Ribs	Gear Rib	Main Gear Loads	Bearing, In-Plane Shea	A		CT	ET	PT		MQT-3, BJT-1, WST-2
		Gear Door Hinge Loads	Bearing, Bending	A			ET			BJT-1,-2
	Actuator Rib	Elevon Actuator Loads	Bearing, In-Plane Shea	A		CT	ET	PT		MQT-3, BJT-1, WST-3
Leading Edge	Slant Surface	Max Stag. Pressure	Normal Pressure (Push)	A		CT				MQT-4
		Tile Pull Test	Normal Pressure (Pull)	A		CT				MQT-4
Spar to Skin		Pull-Up, Max Sub Lift	Peel, Shear	A			ET	PT		AJT-1,-2,-3, WST-1
Spar Web to Spar		Pull-Up, Max Sub Lift	Peel, Shear	A			ET	PT		AJT-1,-2,-3, WST-1
Rib to Skin		Landing, Max Sub Lift	Peel, Shear	A			ET	PT		AJT-1,-2,-3, WST-2
Spar to Rib		All	Peel, Shear, Twist	A			ET	PT		AJT-1,-2,-3, WST-1,-2,-3
Wing Skin to Fuselage		Pull-Up, Landing	Shear, Bending	A			ET		VT	BJT-1,-2, SLT-1
Elevon to Spar		Max Deflection (+/-)	Shear, Bending	A		CT		PT		MQT-3,-4, WST-3

A = Analysis
HD = Handbook Data
CT = Coupon Test
ET = Element Test
AT = Comp. Acceptance Test
PT = Comp. Protoflight Test
QT = Comp. Qualification Test
VT = Vehicle Test

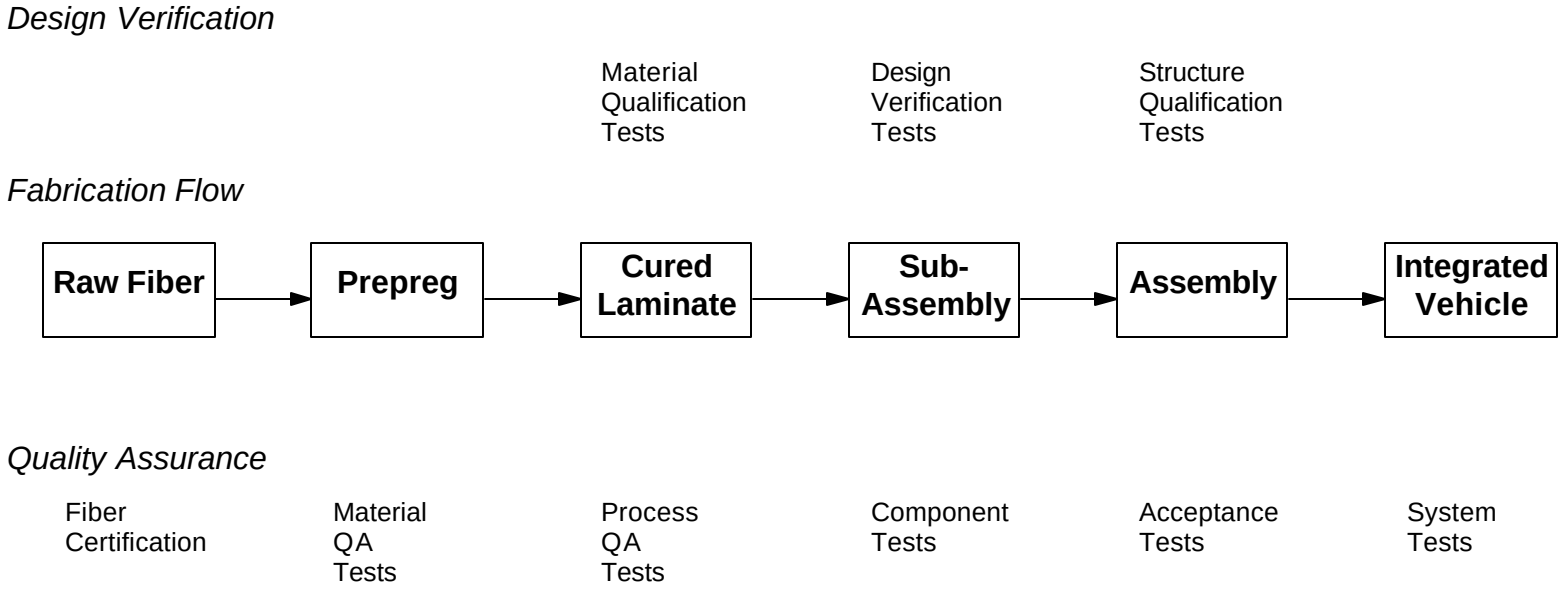
MQT = Materials Qualification Te
HCS = Honeycomb Sandwich P
IPT = Insert Pull Test
AJT = Adhesive Joint Test
BJT = Bolted Joint Test
AWT = Aluminum Weld Test
WST = Wing Static Test
FST = Fuselage Static Test
TST = Tank Static Test
CST = Control Surface Test
CSM = Control Surface Motion T
SLT = Structure Static Loads Te
CCT = Captive Carry Test

Test Sequence	Test ID	Title
Materials	MQT-1	Compression Allowable
Qualification	MQT-2	Tension Allowable
	MQT-3	In-Plane Shear Allowable
	MQT-4	Flex Strength Allowable
Honeycomb	HCS-1	Long Beam Flex
Sandwich	HCS-2	Core Flatwise Tension
Panel	HCS-3	Core/Face Peel

Test Sequence	Test ID	Title
Insert Pull	IPT-1	Pull-Out
	IPT-2	Shear Out
Bolted Joint	BJT-1	Pin Bearing Strength
	BJT-2	Bolt Pull-Out
	BJT-3	Slotted Joint Shear
	BJT-4	Open Hole Compression

Test Sequence	Test ID	Title
Adhesive Joint	AJT-1	Peel Strength
	AJT-2	Lap Shear Strength
	AJT-3	Bending / Peel Strength
Wing Static	WST-1	Pull-Up Load Case
	WST-2	Landing Load Case
	WST-3	Elevon Load Case
	WST-4	Max Torsion Load

Figure 3.10 Design Verification



3.2.6 Non-Destructive Evaluation (NDE)

NDE activities include use of audible "tap testing" and ultrasound on all composite materials including the RP-1 fuel tank. X-ray is also used to look for voids in composite fuselage panels. Traditional dye-penetrant inspection and X-ray techniques are used for all welded aluminum structures, such as the LOX tank.

3.2.7 Software Design and Verification

The philosophical approach to X-34 software development is to develop a very simple set of software modules to control the vehicle during discrete modes of operation. This software is almost entirely of flight proven heritage from the Space Shuttle, Pegasus, and Taurus programs. Software is designed and managed by two separate groups. The guidance, navigation and control (GN&C) team is responsible for all navigation and stability control software. The avionics team handles all non-GN&C-related software.

The X-34 does not employ any specific Mil-Standard or NASA Standard related to software development or independent verification and validation (IV&V). The X-34 program does not have a separate group under contract to provide software IV&V, (nor did the contract include funding for software IV&V.) However it is important to note that much of the X-34 software has a heritage which involved extensive IV&V, namely the Pegasus and Space Shuttle programs. The re-entry and landing is 100% Shuttle heritage. In the case of software under development by Draper Labs, OSC will, in-effect, verify the software through extensive integrated hardware/software testing . It should also be noted that traditional IV&V involves testing at the sub-routine level ("to break the code") and at each successive level of software integration. OSC is not testing down at the sub-routine level but rather focusing on the fidelity of higher level code.

3.2.8 Program Reviews and Action Response Process

Program Reviews

In concert with the "Better/Faster/Cheaper" program development concept, OSC has established a focused program review process tailored to the needs and requirements of the X-34 program. This approach provides for a minimal or reduced set of formalized reviews comprised of the following:

- System Requirements Review
- Outer Mold Line Freeze
- System Design Freeze
- System Verification Review
- Pre-Ship Review
- Pre-Launch Review(s)

The meeting that essentially kicked-off the X-34 program was the System Requirements Review (SRR) conducted in September 1996. The primary objective of this review was to establish system requirements to a level sufficient to allow a design to be formulated and provide the Government with the insight necessary to ascertain the adequacy of the contractor's efforts in defining and allocating the system requirements. To this end the SRR defined system characteristics, identified configuration items, and established the system allocated design baseline.

An Outer Mold Line (OML) Freeze was completed in December 1996. The purpose of this review was to assure that the development of the vehicle aerodynamic configuration was sufficiently mature to allow detailed design of long lead items and construction of wind tunnel models to proceed with minimal risk. The OML Freeze did not represent a detailed systems design review.

A System Design Freeze (SDF) was conducted in May 1997. The scope of this review included a detailed status review of all system/subsystem designs, schedule performance, and all Interface Control Documents (ICD) and specifications. The SDF also reviewed the status of all action items generated at the System Requirements and OML Reviews.

Formal reviews yet to be completed are the System Verification Review, Pre-Ship Review and the set of pre-launch reviews which, as currently proposed, would consist of the following to be conducted prior to each flight:

- Flight Safety Review (L-2 to L-4 weeks)
  - finalize WSMR Flight Safety Operational Plan
  - flight safety oriented
- Mission Readiness Review (TBD)
  - Vehicle preparedness
  - mission success oriented
- Flight Readiness Review (L-1day)
  - Range preparedness

Action Response Process

As an integral part of all formal reviews, an action item identification and response process was established and implemented. This process is principally implemented through the use of the Review Action Recommendation (RAR) document. This document contains the following elements:

- Originator (any participant i.e. Government, academic, industry, etc., who is involved in the particular review)
- Description of issue
- Principal OSC response individual or actionee
- System/subsystem/component of interest
- Recommended action and assignment criteria i.e. accept, modify, combine, close, etc.

The steps to RAR close-out are:

- Responsible Orbital actionee submits RAR status/disposition to X-34 System Engineer
- Closure is accepted/rejected by Chief Engineer and System Engineer
- Rejected RARs returned to actionee for further action
- Closed RARs logged into electronic file system
- Copies of closed RARs sent to MSFC X-34 Chief Engineer
- MSFC X-34 Chief Engineer forwards closed RAR copies to RAR originators
- Originators may request further action if Orbital response was not satisfactory

3.3 Manufacturing and Production-Related SMA Processes

3.3.1 Parts Alert System and Government Industry Data Exchange Program (GIDEP)

OSC is a participating member of the GIDEP. This includes representation from the Dulles, Virginia., Germantown, Maryland., Chandler, Arizona., and Pomona, California. facilities. In general, the OSC participation encompasses all aspects that could have impact or potential impact on OSC flight hardware i.e. review alerts, problem advisories, product change notices, manufacturing sources, and safe alerts.

OSC uses a cross-business-unit team (of three or four people) to examine GIDEP alerts for impact on ongoing programs. This matrixed functional process is consistent with the "Better/Faster/Cheaper" paradigm. Vendor surveys are conducted as required on parts providers.

The GIDEP review process includes a search of the manufacturing databases and traceability databases to determine if there is any match between the suspect parts covered in the GIDEP document and parts used in flight hardware. If a match does exist, then the Flight Assurance Manager (FAM) of the impacted program is immediately notified, along with the parts engineer, and appropriate actions are taken. These actions may include, but are not necessarily limited to, the following:

- remove suspect parts from stockroom stores and/or kits and assemblies in process, or remove from flight hardware.
- parts removed may then be either scrapped, re-screened or re-tested depending on the nature of the alert. Lot sample tests or additional destructive tests may also be performed.
- suspect parts may be replaced with alternative parts or parts from a different manufacturer.
- originator of the GIDEP Alert or the manufacturer of the suspect parts may be contacted for additional information
- other OSC Divisions and OSC subcontractors may be notified for possible impact on their flight hardware.

In addition to acting on information received through the GIDEP system, OSC also reports through the GIDEP system any significant parts problems experienced at OSC or any of its subcontractors. The requirement to establish and implement a GIDEP review is also flowed down to OSC's subcontractors. This flowdown requirement derives primarily from the technical directive document TD-0211 "Standard EEE Parts Plan for Flight Hardware" which requires all subcontractors to have a GIDEP review system in place, and to report any impact on flight hardware to OSC and to take appropriate corrective action as required.

3.3.2 Quality Assurance & Supply Chain Management Process

Performance Assurance Implementation Plan (PAIP)

The PAIP describes the flight assurance functions to be accomplished by OSC for the X-34 test-bed vehicle system. The X-34 test-bed vehicle system comprises the X-34 test-bed vehicle and the carrier aircraft. The objective of the flight assurance function is to assure a high probability of mission success by applying proven techniques to each of the flight assurance tasks. The PAIP specifies the application and implementation of OSC in-house policies and procedures associated with safety, reliability, maintainability, parts, materials and processes, quality assurance, metrology, configuration management, and software assurance.

Quality Assurance

OSC Quality Assurance (QA) provides production support by resolving issues with contractual quality requirements. QA monitors the prime contractors' manufacturing workmanship standards to verify that selected fabrication processes such as welding, soldering, bonding, etc., meet specification. At the receiving and inspection point OSC QA reviews documentation, inspects and tests items, identifies and controls non-conforming items, and protects accepted items. QA provides support to other contract administration functions including:

- production support
- design review support
- assessment of design review processes
- engineering design changes review
- contract waiver and deviation review
- verification that documentation updates are accurate

Supply Chain Management

Increased emphasis is being placed on process verification and evaluating and measuring products to determine conformance to specifications. OSC is conducting pre and post award reviews to determine if suppliers are capable of satisfying quality requirements. As such OSC's supplier quality assurance program is a major contributor to the contractor procurement source review. All OSC prime suppliers are required to meet either Mil-Q 9858 (in the case of parts providers Mil-I 45208) or ISO 9001standards. Each contractor or parts supplier must operate under a Quality Assurance plan approved by OSC. OSC conducts an audit and spot checks on all hardware vendors. OSC provides each supplier with a specification, a statement of work and drawings. OSC relies on their prime contractors to conduct audits on sub-contractors and third tier vendors. If a subcontractor requires a deviation or waiver, the concern is submitted to the Configuration Control Board for review and disposition

ISO-Certification

The current contract with NASA does not require OSC to be ISO 9000-certified. However, the Advanced Projects Group, which manages the X-34 program, receives considerable matrix support from two other OSC organizations: 1) the Space Systems Group (SSG), headquartered in Germantown, Maryland, currently in the ISO-certification process, and 2) the ISO-certified Launch Systems Group (LSG), headquartered in Chandler, Arizona. The SSG also provides all of the calibration services which include documented and controlled measurement standards and a recall system to ensure that all standards and measurement equipment are recalibrated at periodic intervals which directly supports assembly of the X-34 vehicle at the APG assembly facility in Dulles, Virginia.

3.4 Operational Safety (System Safety & Range Safety) Processes

3.4.1 Requirements

As discussed in Section 2.0, OSC will implement the baseline flight test program from the White Sands Missile Range/Holloman Air Force Base (HAFB) complex near Las Cruces, New Mexico. All operations will be conducted over the WSMR. The OSC Flight Assurance manager is responsible for coordinating or orchestrating the ground and flight safety activities related to the X-34 vehicle.

X-34 flight operations are governed by the WSMR Base Commander and the national range universal documentation system. The Range Safety Process is under the control and direction of the Base Commander. The Range Safety Office is responsible for all issues regarding Flight Termination System (FTS) design reliability and redundancy, as well as FTS command-destruct and communication system security.

System Safety & Range Safety Requirements

- X-34 Accident Risk Assessment Report (ARAR), (TD-9110, Rev X2.), contains technical information concerning hazardous and safety critical equipment, systems, and materials used in the X-34. This document is prepared for WSMR Range Safety and HAFB Safety to Review, and will be submitted to WSMR Range Safety and HAFB Safety prior to hardware shipment.
- The ARAR will provide in detail the L-1011/ X-34 hazards.
- The Flight Termination System Report, (TD-9111), provides a detailed flight termination system description, hardware, and test reports.

OSC System Safety Requirements

- Flight systems shall satisfy all negotiated range safety requirements associated with WSMR, HAFB and FAA as required in the following documents:
  - X-34 Design Safety Requirements Document, X60023
  - X-34 Safety Requirements for Ground Operations, X60024
- Flight systems shall be two fault tolerant to any catastrophic event
- No single credible failure or operator error during ground operations shall result in significant personnel Injury or damage to flight hardware.
- X-34 vehicle shall be safe to jettison from L-1011.
- A function whose inadvertent operation could result in a catastrophic event must be controlled by a minimum of three inhibits, whenever the potential exists. At least two of the three required inhibits are monitored.

Hazard Analysis Ground Rules

For purposes of the Hazard Analysis, the carrier aircraft is considered part of the X-34 flight system.
A catastrophic event is defined as either:

- catastrophic damage to carrier aircraft or ground facilities, or
- personnel death.

Catastrophic Damage to the carrier aircraft or ground facility is defined as damage that results in total loss of flight worthiness of the carrier aircraft or major facility damage. credible failure is a condition that can occur and is reasonably likely to occur. Failures of structure, pressure vessels, and pressurized lines and fittings are not credible if they comply with appropriate design margins of safety.

3.4.2 Ground Operations

X-34 pre-flight ground operations take place at HAFB. HAFB provides necessary ground support equipment and implements the OSC ground safety program contained in "Safety Requirements for Ground Operations" X60024, The loading of both liquid oxygen and RP-1 is carried out by WSTF personnel. The NASA White Sands Test Facility, operating under an OSC task agreement, provides LOX safety support.

3.4.3 Captive-Carry Operations

Captive-carry is the term used to describe the mated L-1011/X-34 vehicle. This aerospace flight system must be certificated by the Federal Aviation Administration (FAA) as an experimental aircraft and must demonstrate compliance with applicable Federal Aviation Regulations (FAR's). OSC has retained the services of Marshall Aerospace Ltd. to perform the necessary work to acquire FAA certification. OSC has established a task agreement with NASA Dryden Flight Research Center to conduct the flight testing necessary to demonstrate compliance with FAA requirements.

L-1011/X-34 Aerodynamic Separation Analysis and Verification

Separation Modeling

L-1011/X-34 separation analyses have been completed for the first flight scenario involving drop of the unfueled -unpowered 18,000 lb. vehicle. Analysis and testing continues in preparation for the fueled-powered flight scenarios.

The static vertical margin is 17 inches between the X-34 rudder tip and aft end of the L-1011 fin box. The static horizontal margin between the X-34 rudder and the L-1011 fin box is four inches. Analyses by Nielsen Engineering and Research (NEAR), Palo Alto, California, provided guidance for selecting the optimal drop condition which gives the most clearance margin. OSC conducted independent analyses which verified (and extended) the NEAR assessment. The NEAR aerodynamic model developed for the jettison of munitions ("stores model") has been used successfully to model the drop of the Pegasus air-launched expendable launch vehicle.

X-34 Roll Mitigation at Drop

The X-34 roll autopilot is being used at the time of drop so as to avoid side impact of the rudder given the limited clearance available. Simulations indicate that all lateral (static lateral clearance minimum is 4 inches) impact cases are avoided with the use of the X-34 roll autopilot. Limited impact cases may exist for a roll autopilot failure, however the impact forces calculated would not cause damage to the L-1011 fin box.

Wind Tunnel Testing

A separation wind tunnel test is scheduled for July 27, 1998 in the Calspan (formerly the Cornell Aeronautics Laboratory) transonic wind tunnel located in Buffalo, New York. 1/30th scale L-1011 and X-34 vehicle models will be tested to determine the captive carry and close proximity flow field. The data will be used to run further simulations and build confidence in the nominal separation conditions and drop envelope. Wind tunnel data for control surface deflections corresponding to multiple failures will be gathered to estimate impact forces. At this time the system is two fault tolerant to a control surface hardover at the time of drop. Multiple failures or "non-credible " control surface hardovers are only being given limited evaluation since the probability of their occurrence is very small. NASA Langley Research Center is assisting in test scenario definition, testing and data reduction.

X-34 Propellant and Oxidizer Slosh Mitigation and Analysis

In discussions during the on-site review questions were raised concerning the influence of sloshing partial-fuel-load forces on L-1011/X-34 separation margins. All tanks incorporate slosh baffles to minimize the amount of slosh during flight operations.

No scenarios currently exist in which the X-34 has a partially full RP-1 tank during captive carry operations. Maintaining a full RP-1 tank is also a requirement for (non-launch) point to point transportation across U.S. In the case of liquid oxygen (LOX), a maximum boil-off of 6% is allowed. At the time of drop, the LOX tanks will be between 94 and 100% full. Therefore LOX sloshing could occur if the L-1011/X-34 flight system is accelerating (climbing, descending turning). Current flight rules require the flight system to be stable for approximately

10 minutes prior to drop, imposing no acceleration on propellant or oxidizer. Follow-on discussions with OSC indicate that slosh could possibly be a factor in an emergency jettison scenario where the flight system is not trimmed and stable. It is recommended that OSC consider the emergency release scenario where the L10-11 is maneuvering and LOX boil off has created a 94% LOX load and associated slosh to assure that forces associated with sloshing will not influence separation margins.

Safety Hazard Analysis

During the baseline flight test program, all failure modes of the L-1011/X-34 vehicle will be contained within the bounds of the WSMR. It is important to note that any potential operations from the Eastern Range (OPTF) will require consideration of complex abort scenarios which will require over-flight of populated areas.

In addition to the flight assurance gained through FAA certification, OSC has in-place a corporate level flight system safety directive, which identifies and evaluates safety hazards to the flight crew and technical staff on board to OSC L-1011. These analyses are contained in the ARAR. Development of this document involves development of Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis, and Hazards Analysis. Selected ARAR examples follow:

- Premature Engine Ignition While In Captive Carry

  Hazard
  - Engine ignition while attached to the L-1011 will cause catastrophic damage and loss of life

  Control Features
  - 2 utility controller inhibits : breakwire and firing Field Effect Transistor (FET)
  - 3 monitored inhibits in the Flight Termination Logic Unit (FTLU), breakwire-dependent, with a 2.5 second time delay for safe separation distance.

  Verification
  - functional testing
  - FTLU and utility controller inhibits are monitored by Launch Panel Operator (LPO)

- Premature Engine Ignition After Release Prior To Safe Separation Distance

  Hazard
  - X-34 engine ignition prior to safe separation distance from the L-1011 will cause catastrophic damage

  Control Features
  - FTLU has a 2.5 second time delay for safe separation distance prior to enabling engine ignition relay

- Flight computer needs to sense breakwire prior to starting flight portion of Mission Data Load
- Inertial Navigation System (INS) velocity and attitude must be within proper limits.

Verification
- Functional testing
- FTLU and utility controller inhibits are monitored by LPO prior to release

- Parachute Deployment While In Captive Carry

Hazard
- Parachute deployment while in captive carry could result in L-1011 damage or loss of control

Control Features
- Design is inherently safe. Capture pin must be engaged for chute to be structurally coupled to X-34. Capture pin is not engaged during captive carry
- Flight computer and utility controller inhibits

Verification
- System functional testing
- Flight computer breakwires and utility controller inhibits monitored by LPO and ground controllers.

- Landing Gear Deployment While In Captive Carry

Hazard
- Landing gear deployment while in captive carry could result in L-1011 loss of control and prohibits safe separation of X-34. L-1011 can not safely land with X-34 landing gear deployed

Control Features
- Flight computer and utility controller inhibits
- Launch panel operator (located on L-1011): hydraulic isolation valve isolates the X-34 landing gear from the hydraulic system

Verification
- System functional testing
- Flight computer breakwires and utility controller inhibits monitored by LPO and ground

These examples have been specifically selected to highlight the captive-carry and separation risk issues raised in discussions during the on-site review meeting.

3.4.4 Flight Operations

WSMR Range Safety Management Documentation

The principal WSMR range safety requirements document is "NROCE-991-001 Rev. 1, Flight Termination System (FTS) Requirements Document For The X-34 Technology Test Bed Vehicle." This document, tailored from Range Commanders Council (RCC) 319-92, sets forth the WSMR Range Safety requirements for the X-34 technology test bed vehicle FTS. It outlines the requirements for establishing design criteria, testing, and data submittals. It also prescribes the procedures for FTS flight test approval, approvals of subsequent modifications, and defines the operational authorities and responsibilities. The Safety Engineering Branch (STEWS-NRO-CE), Operations Control Division, National Range Operations Directorate, WSMR , is the range element responsible for resolving problems associated with design, usag,e and test of the FTS at the missile test range.

The identified policies, requirements, and procedures are binding upon the X-34 test program at WSMR, unless specifically amended or waived, in writing, by the Commanding General of WSMR, or his duly authorized representative. The X-34 Program Office, or its duly authorized contractors, are responsible for fulfilling the requirements specified . The compliance with this document does not guarantee the acceptance of the X-34 FTS at other ranges.

Range FTS Approval Process

The Range FTS approval process is a five-phase approach in which (1) the program requirements are identified, (2) an FTS concept is derived which meets program and range safety requirements, (3) a final FTS design is made which functions as per the concept, (4) the design is qualified for use through a series of design verification tests and (5) the FTS is approved for use at the Range following the approval of all operational, test, and checkout procedures.

FTS approval must be obtained 60 days prior to the start of flight test operations. This approval will be granted following satisfactory fulfillment of the requirements specified herein. Satisfactory performance in these requirements is determined by the WSMR Safety Engineering Branch, (NRO-CE), Participation by this organization during all phases of the concept, design, approval, qualification testing, pre-test, vehicle build, ground pre test and flight test is required. Level of Range participation in these activities will be determined by the Range . After approval, continued coordination must be maintained to ensure that any modifications still result in an approved FTS for use at the Range.

The following is a summary of the requirements that the X-34 will have to meet prior to gaining approval:

FTS Reliability

The overall FTS reliability must be demonstrated. The overall system reliability of the FTS shall be 0.999 at 95% confidence level. FTS reliability may be demonstrated by meeting the

following four requirements:

- Designing the FTS to be fault tolerant.
- Performing Range approved qualification, acceptance, certification, and pre-mission testing.
- Maintaining stringent quality control as required by MIL-STD-973, *Configuration Management,* 24 Nov 93, reference 2.2h, or other acceptable quality control specification agreeable to the Ranges.
- Performing a reliability prediction on the FTS to show the 0.999 probability is met. The mission time used in the reliability predictions shall include a minimum of 150% of the predicted flight time and shall be verified by analysis in accordance with the Parts Stress Analysis of MIL-HDBK-217E, *Reliability Prediction of Electronic Equipment*, reference 2.3, using the applicable environmental factor.

Flight Termination System Report (FTSR)

To obtain final FTS approval by the Range, and prior to the first vehicle flight, the user must provide a final FTSR that contains the following data items:

- A detailed narrative description of the FTS;
- Detailed FTS schematics and wiring diagrams;
- FTS component specifications;
- QA procedures and reliability documentation;
- Antenna patterns;
- Link Analyses;
- Battery Load Analyses;
- Environmental Analyses;
- Bent-Pin Analyses;
- FMECA;
- Qualification test plans/procedures/reports;
- Acceptance test plans/procedures/reports;
- Failure analyses reports (if applicable);
- Certification test procedures/reports;
- FTS assembly and checkout procedures;
- Modifications (if applicable);
- Waivers granted (if applicable).

FTS Design Configuration

The FTS shall be redundant to the maximum extent possible, and shall include the following components: Dual UHF flight termination receivers (FTRs), FTS antennas and coupler, independent, redundant FTS battery power system, redundant independent Flight Termination Logic Units (FTLU), appropriate end items, circuitry interconnecting these components, and the

control/monitoring circuitry and equipment.

- Independence. The FTS shall be independent of all other vehicle systems except where agreed upon by the Range.

- Accessibility. The FTS circuitry shall be configured to be field testable requiring minimum disassembly. Design should accommodate easy replacement of FTS components where such is likely to be required.

X-34 FTS Performance Characteristics

The FTS must be able to be activated by:

- A commanded signal which engages a prescribed sequence of modulating Inter-Range Instrumentation Group (IRIG) tones.
- The FTS Action 1, must result in shutdown of the vehicle main propulsion unit.
- The FTS Action 2, must result in placing the vehicle into an unstable attitude which produce zero lift, zero yaw, and zero thrust.
- These actions, shall be independent and configured to afford their usage at the discretion of the Range Safety Officer.

Pre-Flight Readiness Review Process

The following reviews will be conducted prior to each flight:

- Flight Safety Review (L-2 to L-4 weeks)
  - Finalize WSMR Flight Safety Operational Plan
  - Flight safety oriented
- Mission Readiness Review (schedule TBD)
  - Vehicle preparedness
  - Mission success oriented
- Flight Readiness Review (L-1day)
  - Range preparedness

These reviews are a sub-set of the overall X-34 program review process described in Section 3.2.8 of this report.

Between-Flight Safety Assurance Processes

The integrated vehicle health monitoring system, which, together with rapid software reprogramming, will make possible the quick turnaround of the X-34 vehicle. As previously noted, this is a major demonstration goal.

The philosophy for accomplishing turnaround validation/checkout is to evaluate vehicle performance via telemetry information and generate any required Field Discrepancy Reports (FDR's) based on this data. The FDR is used to document troubleshooting, and, in conjunction with existing procedures, to remove and replace hardware. In addition, a visual inspection of the vehicle external surfaces, and internal cavities will be performed and discrepancies and repairs documented in FDR's.

Operations will perform functional testing at the subsystem level following vehicle maintenance and repairs during each turnaround. This functional testing will be performed as a "Vehicle Verification" test which will use the flight computer to verify the functionality of each avionics, hydraulics, pneumatics, and MPS component on the vehicle. In effect, if the avionics system interfaces with a component, then that interface and the functionality of the component is verified. The remainder of the hardware will be serviced on a periodic basis. The selection of periodic validation/checkout intervals, will be through subsystem/hardware analysis results, failure history and the disposition and corrective action implementation of prior failures. The X-34 structural and subsystem inspection task will be performed each turnaround or until a damage tolerance has been developed to satisfy the program. The major forms of damage considered during the initial phase of the program are:

- Fatigue/Dynamic load damage
- Environmental deterioration or damage
- Accidental damage
- Thermal Damage or degradation

Software will be validated by "hardware in the loop" testing following any modification to the flight software load.

The FASTRAC engine will be removed after each powered flight. Contamination control measures to be defined by the MSFC/FASTRAC engine program will be implemented to protect the main propulsion system plumbing, valves and tanks. It is anticipated that a positive pressure purge method will be employed. NASA WSTF (under a task order agreement with OSC) will be defining the LOX servicing/contamination prevention requirements which would be implemented between flights. Installation of a new engine will be conducted in accordance with MSFC/FASTRAC engine program defined requirements.

Payload Safety Review Process

Payload safety is governed by X-34 project documents X60023 and X60024. These requirements include pre-ship payload safety reviews as well as a formal payload hazard analysis. The review board is chaired by the X-34 Flight Assurance manager.

3.4.5 Range Safety Working Group

OSC Flight Assurance Manager and the WSMR Range Safety Officer co-chair this working group. This team conducts weekly telecons and provides a forum to identify, document and track work items necessary to fulfill range safety requirements. An example from the Range Safety Working Group Log is shown below.

3.4.6 Emergency Response Planning Process

WSMR and HAFB require that a emergency response plan be developed for all tests. OSC plan addresses emergency situation during ground, flight , and test operation. Test coupons of the composite structure will be burn tested to obtain additional information concerning hazards associated with smoke. This information will be included with the Material Safety Data Sheets (MSDS) to represent the greatest hazard chosen and used to represent the entire vehicle. Training will be provided to WSMR and HAFB crash and fire rescue personnel by OSC for familiarization with X-34 and location of hazardous components. Existing training course for the L-1011 safety will be conducted by the L-1011 Flight Engineer with safety and emergency response personnel at HAFB, WSMR, and NASA White Sands Test Facility (WSTF) following the L-1011 arrival for the first flight. Contingency procedures will be modified to include the L-1011 with X-34 attached. Lesson learned from the NASA, DC-XA, Clipper Graham mishap contributed to the development of this plan.

3.5 FASTRAC Engine - SMA Support

The FASTRAC 60K engine is being designed and built by MSFC and will be provided as GFE to OSC for the X-34 Program. FASTRAC was conducted in accordance with ISO 9001 requirements. Four engines will be built for testing by Stennis; the flight engines will be built and shipped to OSC. The FASTRAC 60K engine development is being implemented by Product Development Teams (PDTs) at MSFC. MSFC SMA is supporting the development through membership on the PDTs. MSFC SMA prepared a Quality Plan for the FASTRAC engine which gives the quality requirements, based on MSFC quality system, for processing and acceptance of hardware and test verification. Along with the Quality Plan, MSFC SMA prepared an Inspection and Testing Plan for the FASTRAC engine. This document specifies the inspection and test requirements that will be required for the acceptance of FASTRAC Engine hardware. MSFC SMA prepared a Risk Management Report for the test engine. This report presents a new concept for combining hazards, failure modes and effects, and critical items into a single document. A separate Risk Management Report has been prepared for the flight engine and will be updated as required by the engine test program. These risk management reports have been/will be provided to OSC. MSFC Safety and Quality approve drawings and documentation for initial release, as well as changes as CCB members. MSFC SMA has also provided safety and quality inputs to the Engine Hot-Fire/Test Specification development and will support these tests.

3.6 Main Propulsion System (MPS) - SMA Support

MSFC, through a task agreement with OSC, is designing the MPS for the X-34 program. MSFC will design the MPS and provide the drawing/documentation package to OSC. MSFC SMA will continue to provide the necessary support for this task. This support includes quality and safety inputs to the design, review and approval for drawings and documents, and CCB membership. MSFC has also prepared a Risk Management Report for the MPS which combines hazards, failure modes, and critical items into one document.

4.0 X-34 Safety and Mission Assurance Issues

4.1 System Safety

Flight safety issues were discussed at length during the on-site review. It can be expected that continuing, and expanded SMA insight will be required as the program moves to the optional flight test program.

Heritage Software Concerns

It noted that while L-1011/Pegasus heritage supports the development of captive-carry hazards analyses, and extreme care should be used to avoid over-reliance on this heritage, as the X-34 represents a new and unique configuration.

Flight Safety During Captive Carry Operations

Questions have been raised concerning L-1011/X-34 catastrophic failure modes including premature or inadvertent drop during captive carry, post separation collision, and premature engine ignition. OSC and MSFC SMA must maintain a high level of rigor in documenting analyses and testing necessary to support development of risk acceptance rationale.

FAA Certification of L-1011/X-34

Increased insight is required (on the part of NASA) to better understand the processes involved in FAA Certification of L-1011/X-34. Marshall Aerospace Ltd. is under contract to OSC to acquire FAA certification. DFRC is the subcontractor to OSC to manage FAA certification testing. The NASA FASTRAC engine program is on the critical-path to furnish information necessary to acquire certification. Difficulties have been encountered over the past six months in communicating required data in a timely fashion. Issues have also been raised concerning how OSC will demonstrate compliance with pressure vessel safety requirements necessary to satisfy Federal Aviation Regulations (FARs). OSC is using Mil Standard 1522 as the standard for X-34 pressure systems to meet FAA certification requirements, (although FAA does not specifically require compliance with Mil Standard 1522). OSC has also indicated concern with traceability and insight into the FASTRAC engine development. NASA and OSC managers must better communicate and coordinate on issues related to FASTRAC safety and mission assurance.

4.2 Staffing Levels for SMA

The X-34 program Flight Assurance organization is operating at a minimum staffing level, comprised of three full-time professionals. This lean approach renders the program potentially vulnerable to unexpected events. While viewed as a percentage of the overall X-34 program staff (5%), the SMA staffing is comparable with larger programs. This may be a misleading

perspective however as implementation of the required SMA task-set requires a finite or minimum number of professional staff. Therefore, embedded risks exists in the potential for compromising SMA process implementation by over-burdening SMA staff. Corporate OSC resources should be available to bolster, as necessary the SMA (Flight Assurance) functions in the X-34 program. NASA MSFC X-34 program management and SMA management should be vigilant in assuring the effectiveness of SMA process implementation. The OSC Flight Assurance full-time staffing should be expected to increase if the program implements the optional flight test program.

4.3 Potential Eastern Range Operations

The X-34 program will face a variety of new and different requirements for operations off the east coast. For example, the Eastern-Western Range (EWR-127) requires parts traceability for FTS components while the WSMR does not impose this specific requirement. Hardware changes will be required. The X-34 will have a nominal mission trajectory that is completely within U.S. military coastal restricted areas, however, some East Coast abort sites will involve overflight of populated areas. The environmental assessment process and the range safety hazard analysis will become more complicated (and more contentious). OSC will most certainly have to increase the X-34 Flight Assurance staff to accommodate the increased work load. NASA/MSFC SMA management should work to acquire insight into the advanced planning for the optional flight test program operations.

4.4 Baseline X-34 Flight Termination System (FTS)

X-34 Flight Termination System Hardware

OSC has purchased the FTS receiver from Herley-Vega (HV) as recommended by the White Sands Missile Range (WSMR). HV receivers have been in use at WSMR since 1990. While this receiver has a long record of demonstrated flight success, HV uses commercial manufacturing practices where parts traceability and documentation is not a standard service. Note that the absence of parts traceability may represent an issue for the certification of the HV-FTS on the Eastern Test Range because of EWR 127-1 requirements for 100% parts traceability.

X-34 Flight Termination Process

The X-34 flight termination process involves two steps. The first FTS up-link command, "engine cut-off", closes the engine valves which shuts down the propulsion system. With engine shutdown the flight computer autonomously sends commands to dump remaining fuel and oxidizer. The X-34 continues to operate under autonomous internal guidance/navigation and control software and has the opportunity (5 to 8 seconds) to correct the errant trajectory. If the vehicle fails to recover, a "terminate" command is transmitted resulting in an "energy dissipation mode" , where there is no net lift, and the vehicle assumes a ballistic trajectory. This is

accomplished by a high pressure helium system which simultaneously drives the port elevons (control surfaces) up, and the starboard elevons down.

4.5 Flight Termination System Communication Security Issues

The issue of inadvertent or intentional interference with FTS (and/or command and control up-link) has been raised in recent discussions with the NASA Inspector General (IG). This issue relates not only to the X-34, but to other X-vehicles and space flight programs.

The NASA Inspector General (IG) has recommended implementation of a high security FTS command/destruct decoder-initiator system and an equally secure command uplink system. Tampering, spoofing (jamming or misdirecting) or other intentional interference with the FTS could result in destruction of the vehicle during nominal operation or impairment of range safety's ability to terminate flight in the case of an errant ground track.

Secure FTS

Command Receiver Decoder (CRD) receives signal, decodes signal, and initiates termination function. Ground-based Command Transmitter System (CTS) generates, modulates, and transmits the signal. Differences between secure and non-secure systems involve: 1) destruct command generation in the CTS and 2) decoding of the destruct command on-board the vehicle. The IG indicated that a cost increase on the order of $85K to $120K would be associated with implementation of secure system hardware. Additional costs would be associated with program compliance with security control and handling requirements.

Range Safety and FTS Responsibilities

Acknowledging NASA and OSC's shared responsibility for assuring public safety, the military test range Base Commander nonetheless has ultimate responsibility for any vehicle launched from his/her facility. The Base Commander delegates range safety responsibilities to the Range Safety Office which addresses issues related to:

- Flight Termination System (FTS) hardware design
- FTS software
- Flight hazard and public safety

The X-34 program will need to work with the White Sands Missile Range Safety Office for operations in New Mexico, and the USAF, 45th Space Wing, for operations based at Kennedy Space Center. Range safety requirements for KSC operations are contained in EWR 127-1. Range safety requirements for WSMR are contained in RCC-319-92, and special RLV revision, NROCE-991-001 rev.1, "Flight Termination System (FTS) Requirements Document for the X-34 Technology Testbed Vehicle."

Scenario 1: The "Casual Hacker" Threat

Threat Scenario

This scenario presented by the IG involves an individual using the internet to discover information concerning the FTS manufacture and design specifications, including default tone settings. The non-secure FTS receiver has up to five tones available for identity/authentication access necessary to enable command. In reality only a two tone code is typically employed.

The Casual Hacker could then acquire a relatively inexpensive (several hundred dollars) radio transmitter and associated hardware, (power supply etc.) and be capable of sending unauthorized commands and/or jamming or spoofing the FTS receiver.

Risk Mitigation

This potential threat was discussed with OSC avionics and operations Team Leads during SMA review background technical meetings on May 6 and 7, 1998. The following mitigation measures (already in place) were identified as more than adequately addressing the Casual Hacker scenario.

- Range frequency control officials at WSMR are continually monitoring all radio frequency (RF) transmissions in and around the WSMR. Any unauthorized transmission (on any frequency) would immediately be identified, located and addressed by security personnel. Any unauthorized transmission would cause the range to immediately assume a "Red" (cease operations) status.

- Range flight termination system receivers on the X-34 vehicle would not be turned on until the X-34 flight operations manager was instructed by the Range Safety Officer (RSO) to do so. Prior to issuing this clearance the RSO would confirm that the X-34 vehicle was "saturated" with RF radiation from the powerful range safety antenna system, radiating 600 to 1000 watts of RF power. This level of power will preclude the successful intrusion of a lower power level (unauthorized transmission) into the FTS receiver detector.

- Once "locked-up" by the range safety RF system the X-34 FTS receiver automatic gain control (AGC) and noise detection electronics would reject any lower wattage transmission on the FTS carrier frequency. It was described as a "signal-to-noise" struggle which the range safety would always win.

- The X-34 FTS communication system will also provide a continual downlink of telemetry to the RSO, providing verification of FTS receiver RF saturation. In the

event of anomalous receiver operation prior to drop, the range would immediately move to a "Red" status.

Scenario 2: The Sophisticated "Bad-Guy" Threat

Threat Scenario

This threat would involve RF attacks launched by a nation or organization capable of radiating hundreds or thousands of watts of RF power from an undisclosed/undiscovered location for presumed political purposes.

This scenario was discussed during the SMA review conducted earlier this year at the Lockheed-Martin Skunkworks facility near Palmdale California. Clear differences of opinion existed between the NASA IG communication security experts and the Edwards Air Force Base range safety personnel concerning the existence of a credible security threat to operations on the California/Utah/Montana test range.

Risk Mitigation:

Secure FTS system including receiver/decoder and up-link encryption provides the most obvious means of mitigating this threat scenario. In the case of the X-33, the review team and the X-33 program mutually acknowledged that additional mitigation measures (i.e., secure FTS system deployment) would be appropriate if a credible threat was present.

Resolution of X-34 Risk Management Issues Concerning FTS

The NASA OSMA review team recommends that the X-34 program management team should work with the NASA Office of Security (Code J), and the NASA Inspector General (Code W) to assess the need for a secure FTS system to support on-range, flight operations in New Mexico.

A separate risk management process (involving Code J, Code W, the KSC operations, and the US Air Force, 45th Space Wing) should be employed to address east coast operations involving a 2000 mile, off-shore, flight corridor, ranging from Wallops Island, Virginia, to Cape Canaveral , Florida. The east-coast scenario presents a different set of signal-to-noise ratio issues, with longer distances from range RF transmitters to the vehicle, and reduced abilities to control unauthorized RF emissions. While the Casual Hacker threat would be largely precluded by off-coast, long range operations it could be argued that a sophisticated attack scenario (assuming such a threat exists) using ship-based, high-power, RF transmitters would have greater opportunity to succeed.

4.6 Design, Engineering and Management System Security

The X-34 program employs a design and engineering data base which is available to industry and government partners by way of a password protected FTP-internet site. The information contained in this data base is read-only. It is also important to note that the internet accessible CAD (computer aided design) environment is in a support role to a more traditional printed drawing system which is maintained under internal OSC configuration control.

Information security is an element in the overall mission success equation. While the X-34 program does not have a formal information security plan in-place, it does employ, basic computer management system security practices. It is acknowledged that an intensive technical review of information security measures, while beyond the scope of this review and report, may provide opportunities for enhancement. The X-34 program management team is encouraged to consult further with the NASA Inspector General and Office of Security on this matter.

5.0 Achieving Safety & Mission Assurance Insight

5.1 Oversight/Insight Methodology

The NASA MSFC SMA insight role is unnecessarily complicated by inherent conflict in assigning a single individual to simultaneously assume three oversight/insight roles:

- sub-contractor to OSC on the Main Propulsion System development;
- insight-consultant to the NASA X-34 program manager (over OSC), and
- oversight to the MSFC FASTRAC engine program (the engine being provided as Government Furnished Equipment to OSC).

It is recommended that the MSFC SMA Director work with the X-34 program manager, the FASTRAC Engine program manager, the Main Propulsion System program manager, and OSC to develop an approach for assuring smoother and more effective implementation of SMA oversight/insight responsibilities.

5.2 MSFC SMA Staffing

The MSFC/SMA office should consider amending their Annual Operating Agreement (AOA) to identify the required resources necessary to effectively carry out their oversight/insight roles related to the X-vehicle programs.

5.3 FASTRAC SMA Support

It was also noted that NASA MSFC/SMA should work with the FASTRAC and X-34 program management to arrange for program funding of SMA tasks (FMEA, Hazards Analysis and Critical Items List) currently being funded through NASA Headquarters research and development funding sources.

5.4 X-34 SMA Ongoing Insight

The X-34 SMA insight support should focus immediate attention on the following processes and issues:

- Range Safety Working Group (participation in meetings and telcons)
- Optional Flight Test Program planning
- L-1011/X-34 Captive Carry issues including FAA certification
- FTS issues including design, reliability, FMECA, and communications security
- Understanding X-34 program information system security issues

6.0 Summary and Conclusions

6.1 X-34 Safety and Mission Assurance Processes

The review team found evidence that rigorous safety and risk management processes were being employed by OSC throughout the X-34 program.

6.2 NASA Safety and Mission Assurance Insight Process

As discussed in Section 5.1, NASA/MSFC SMA, X-34 and FASTRAC program managers should move quickly to address organizational issues which will allow NASA to more effectively acquire process level insight/oversight into the X-34 program elements.

Expectations for ongoing insight include the following:

- Assure that SMA goals and responsibilities known and well understood by all members of the program team.
- Assure life-cycle implementation of demonstrated, stable, capable and controlled SMA processes.
- Assure that effective communication takes place among all members of the program team.
- Verify OSC Flight Assurance presence in all X-34 risk management forums
- Facilitate increased cooperation in FASTRAC engine integration activities.
- Maintain vigilance in monitoring numerous SMA related task agreements
- Maintain vigilance in monitoring suppliers
- Assure that proper SMA staffing levels and skill mix exist
- Implement measures to assure that heritage software and hardware are subjected to rigorous testing which reflects expected operating environment

Further, the review team recommends that the NASA MSFC SMA insight support personnel:

- Participate in Range Safety Working Group activities
- Monitor planning associated with transition from the baseline flight test program to optional flight test program
- Participate in FTS redundancy deliberations and discussions
- Acquire increased understanding of L-1011/X-34 system safety issues.

6.3 Observations/Recommendations

Specific recommendations offered by the review team members:

- OSC should include the Flight Assurance manager in the monthly NASA briefings where cost, schedule, programmatic and safety risk trades may be discussed.

- OSC should document the probability and impact of risks in the Watch List and elevate safety issue visibility.

- OSC should consider introducing a more rigorous and better defined protocol for risk ranking

- OSC should introduce a "safety" check-block in the Programmatic Impacts field of the Issues/Decision Log.

- The X-34 program management team should work with the NASA Office of Security (Code J), and the NASA Inspector General (Code W) to assess the need for a secure FTS system to support on-range flight operations in New Mexico. Additional discussions should be conducted to evaluate the need for secure FTS in the optional flight test program.

- The NASA X-34 Program Office and OSC should ensure that all RARs are (or have been) appropriately dispositioned specifically with regard to confirming closure with the originator of the RAR. There have been some indications that this close-out process has not been completely successful.

- OSC should assess potential risks associated with emergency release of the X-34 while the L10-11 is maneuvering and LOX boil off has created a 94% LOX load allowing slosh. Analyses should verify that forces associated with sloshing will not influence separation safety margins.

6.4 X-34 Program Commitment Agreement (PCA)

The complexity of the operational scenario and the extent to which safety responsibilities are delegated through Task Agreements led some observers at the May 22, 1998 on-site review to question whether or not the chain of responsibility for operational safety was clearly understood. In order to re-emphasize the chain of accountability for safety and the responsibility and to underscore the need for insight into X-34 processes and issues, the review team recommends that the next revision of the X-34 PCA be modified to include a new paragraph as follows:

> ***Safety and Mission Assurance Insight***
>
> *The NASA Associate Administrator for Safety and Mission Assurance is responsible for maintaining insight into issues affecting flight safety, public safety, and mission success. The X-34 Program Manager and Enterprise Associate Administrator remain ultimately responsible for assuring safety and managing program risk.*

6.5 Conclusion

Implementation of the recommendations outlined above will enhance the likelihood of mission success and provide assurance that risks to public safety have been appropriately addressed. The increase in SMA insight will also provide the depth of understanding and level of confidence necessary for NASA to support X-34 launch and flight operations.

Appendix A

SAFETY AND MISSION ASSURANCE REVIEW
SIGN IN SHEET / MAY 22, 1998

Name & Title	Organization & Mailing Address	Phone Number	Facsimile Number	E-Mail Address
Bob Lindberg X-34 Program Manager	Orbital	703-406-5441	703-421-2057	lindberg.bob@orbital.com
Curt Shoffner X-34 Deputy Program Manager	Orbital	703-406-5733	703-421-2057	shoffner.curt@orbital.com
Bob Mercure X-34 Oversight	NASA HQ Code RT	202-358-4599	202-358-3557	rmercure@nasa.hq.gov
John Tinsley KSC X-34 Program/Project Mgr	NASA/KSC MM-B	407-867-4553	407-867-4812	John.Tinsley-1@msc.nasa.gov
Antonio Elias Orbital APG G.M.	Orbital APG	703-406-5514	703-406-3509	ae@orbital.com
Fred Gregory AA OSMA	NASA HQ Code Q Washington, D.C. 20546	202-358-2406	202-358-2699	fgregory@hq.nasa.gov
John London	RA30	256-544-0914	256-544-4301	John.London@msfc.nasa.gov

X-34 Prg. Mgr.	Marshall Space Flight Center			
Steve Newman NASA/HQ/QE	NASA/HQ/Q	202-358-1408	202-358-2778	snewman@hq.nasa.gov
Claude Smith NASA/HQ/QS	NASA/HQ/QS	202-358-1675	202-358-3104	csmith1@hq.nasa.gov
James Lloyd, Director Safety and Risk Management OSMA	HQ NASA Code QS	202-358-0557	202-358-3104	jlloyd@hq.nasa.gov

participants page 2

Name & Title	Organization & Mailing Address	Phone Number	Facsimile Number	E-Mail Address
Yvonne Brill Aerospace Safety Advisory Panel (ASAP)	HQ NASA Code Q-1			
Norris V. Krone Aerospace Safety Advisory Panel (ASAP)	HQ NASA Code Q-1	301-345-8664	301-345-7305	krone@urf.com
Norm Starkey Exec. Director ASAP	NASA HQ Code Q-1	202-358-4453	202-358-2776	nstarkey@hq.nasa.gov
Richard D. Blomberg Chair Aerospace Safety Advisory Panel (ASAP)	HQ NASA Code Q-1	203-323-8464	203-964-0799	rblomberg@aol.com

Dave A. Haynes X-34 Chief Engineer	NASA MSFC	757-864-8214	757-864-4449	d.a.haynes@larc.nasa .gov
Mike Allen X-34 Deputy Prg. Mgr.	NASA/MSFC RA30	256-544-5611	256-544-4103	mike.allen@msfc.nasa.gov
Mike Weeks X-34 Asst Mgr	NASA/MSFC RA30	703-406-5788	703-406-2116	weeks.mike@orbital .com
Ed Kiessling Deputy Director MSFC S&MA	NASA/MSFC CR01 MSFC, AL 35812	256-544-7421	256-544-2053	edward.kiessling@msfc.nasa.gov
James Hatfield S&MA Manager	NASA@MSFC CR85	256-544-0217	256-544-5858	james.hatfield.msfc.nasa.gov
Ed Trentham S&MA Lead	NASA MSFC CR85	256-544-0667	256-544-5858	ed.trentham@msfc.nasa.com
Wayne Frazier Mgr. System Safety	NASA Hqs Code QS	202-358-0588	202-358-3104	wfrazier@hq.nasa.gov

participants page 3

Name & Title	Organization & Mailing Address	Phone Number	Facsimile Number	E-Mail Address
Wilson Harkins R&M Engineer	NASA HQ Code QS	202-358-0584	202-358-3104	wilson.harkins@hq.nasa.gov
Pete Rutledge Rish Mgr. Lead	NASA HQ Code QS	202-358-0579	202-358-3104	pete.rutledge@hq.nasa.gov
Chuck Larsen Systems Engr. Team Leader Space Systems Development	FAA/AST-100/Rm 331 800 Independence Ave, SW Washington, D.C. 20591	202-267-7908	202-267-5463	chuck.larsen@faa.dot.gov

Div				
Richard Kutyn Flight Assurance Manager	Orbital	703-406-5690	703-421-2057	kutyn.richard@orbital.com
Larry J. Baca Assistant Flight Commander Space Planes Operations	586 Flight Test Squadron/DOS 991 Dezonia Drive Holloman AFB, NM 88330	505-679-1443 or 505-475-1210	505-679-1389 or 505-475-1023	lbaca@mailgate.46tg.af.mil
Leonard Donohe General Engineer White Sands Msl Rng Flight Safety	STEWS-NRO-CF WSMR Bldg 1530 White Sands, NM 88005	505-678-7996	505-678-8459	donahel@wsmr .army.mil
Frank A. Chavez Chief, Safety Engr	U.S. Army WSMR White Sands Missile Range, NM 88002	505-678-8613	505-678-3795	chavezf@wsmr .army.mil
Linda Buhl Config Analyst	Orbital - Dulles	703-406-5366	703-406-3562	buhl.linda@orbital .com
Teresa Anaya X-34 Project Engineer, WSMR	White Sands Missile Range STEWS-MT-SB WSMR, NM 88002	505-678-6709	505-678-0689	tanaya@mt.wsmr .army.mil

participants page 4

Name & Title	Organization & Mailing Address	Phone Number	Facsimile Number	E-Mail Address
Bill Jackson	NASA SW IV&V	304-367-8215	304-367-8375	jackson@ivv.nasa.gov

	100 University Dr. Fairmont, WV			
Tom Palo 45 Space Wing Systems Safety	45 SW/SESS 1201 Minuterman St. Patrick AFB, FL	407-494-3285	407-494-6535	tom.palo@pafb.af .mil
Roger DeVivo 45 SW/Flight Analysis	45 SW/SEOE 1201 Minuterman St. PAFB, FL 32905	407-494-5845	407-494-6955	roger.devivo@pafb.af.mil
G. David Low LSG S&MA	Orbital - Dulles	703-406-5554	703-406-3502	low.david@orbital.com
Dan Ridge Office of NASA OIG	NASA HQ OIG 300 G St. NW Washington, D.C.	202-358-1901	202-358-2990	dridge.@hq.nasa.gov
Jack Symanek Telecommunications Specialist	NASA HQ OIG Code W Washington, D.C.	202-358-2455	202-358-2990	jsymanek@hq.nasa.gov
Peggy Evanich	NASA HQ/QE			
Sally Richardson	Orbital/SE	703-406-5498	703-421-2057	richardson.sally@orbital.com
David Grossman SW	Orbital	703-406-5420	703-406-2057	grossman.david@orbital.com
Eileen Brown	NASA MSFC	703-406-5787	703-406-2116	
Tish Donohue	Orbital	703-406-5098	703-421-2057	

Appendix B
Major X-34 Program Milestones

ID	X-34 Activity	1996			1997				1998				1999				2000				2001				
		Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
1	Program Award	8/28																							
2	SRR	9/26																							
3	OML Freeze		12/17																						
4	SDF				5/21																				
5	A-1 Structural Assembly				4/28					5/22															
6	A-1 Static Load Tests								5/25		8/14														
7	A-1 Mass Sim Installation								5/25			10/16													
8	GVT									11/4			12/22												
9	CCT										1/8		2/11												
10	A-2 Structural Assembly								5/25			9/16													
11	A-2 Static Load Tests									9/17		10/28													
12	A-2 Subsystem Integration									10/20			1/28												
13	A-2 Flight Preparation										2/15		3/10												
14	1st Flight, Unpowered												3/11												
15	Static Fire												6/16		6/24										
16	2nd Flight, Powered															8/6									
17	A-3 Build-up												12/1					10/15							

Appendix C

Aerospace Safety Advisory Panel Comments and Assessment

Memorandum

To: ASAP Members and Consultants **Date:** June 2, 1998

From: ASAP X-34 Group - Richard Blomberg, Yvonne Brill, Norris Krone

Subject:X-34 Safety Review - 22 May 1998 at Orbital Sciences Corporation, Dulles Virginia

General

As with the previous X-33 review, the Aerospace Safety Advisory Panel was invited to attend a Code Q safety review of the X-34 that was held at the Orbital Sciences Corporation (OSC) facility on May 22, 1998. In attendance in addition to the contractor were the ASAP members (as shown above), ASAP executive director, representatives of Marshall (MSFC), Kennedy (KSC), the White Sands Missile Range (WSMR), the FAA and NASA Headquarters personnel.

The meeting began with an introduction by Fred Gregory outlining the Code Q need to have a complete understanding of the program so that a recommendation could be made to the Administrator about possible indemnification for the contractor. The agenda followed the thorough outline prepared by the Code Q review coordinators in cooperation with OSC.

NASA funds the X-34 program, and NASA is also a "subcontractor" to provide the FASTRAC engine as GFE. The X-34 will be air launched from the OSC Lockheed L-1011 aircraft. This is the same aircraft they use for Pegasus launches. The first drop will be unpowered, but subsequent flights will fire the X-34's rocket engine.

Overall, the briefing provided a thorough look at the top level development and test activities for the X-34. The depth of the presentations on key safety issues, however, was sometimes lacking. In addition, some key issues were not addressed at all. While none of the issues appeared to be "show stoppers," there were several that warrant additional probing by Code Q and/or the Panel. Overall, in spite of the title "X-34 Safety and Mission Assurance Review" the presentations did not really address much about safety of flight. This is somewhat worrisome for a program with a schedule that indicates it is approximately nine months prior to first unpowered flight and a year before powered flight. The mission assurance discussions appeared to be focused on programmatic risk considerations rather than safety risks.

The charts presented for various programmatic control topics, such as the "watch" list and risk ranking methods, configuration management and flight assurance requirements, tie the parameters together nicely and create the impression that the Orbital Sciences engineering staff has things under control. Commendable in their configuration control discussion was mention that five unincorporated engineering change notices (ECNs) accumulated against a specification triggers a specification revision.

One programmatic area was a bit striking. The Issues/Decision Log OSC uses as part of its program control has no acknowledgment of safety risks as having programmatic impact. There simply is no category for "safety" on the form. When this was mentioned at the meeting, OSC acknowledged it as a shortcoming and said they would add a category. It would be good for Code Q to follow up on this as part of future contacts.

Also, OSC appears to use a reasonable system of subjective risk ranking as part of their risk management system. This is perfectly reasonable. However, there was no discussion of how the subjective system was structured and what efforts are made to ensure that the subjective judgments are reliable. This might be investigated further by Code Q as part of their assessment of the soundness of the risk management approach.

Potential Safety Issues

Both the large number of subcontractors on this program (30) and the fact that no detailed integration and test plans for the X-34 hardware prior to flight were outlined by the presenters are unsettling from the safety standpoint. NASA should ask for detailed integration and test plans for both the unpowered and powered flight vehicles. OSC stated they were acting mainly as the systems integrator on X-34. To ensure safety of flight, contractor/subcontractor responsibilities need to be clearly spelled out, which they were not. Need for clarification exists in the areas of: OSC's responsibilities for hardware quality assurance, which components are subjected to quality and acceptance inspections at the vendor's plants, and what controls are placed on GFE (particularly the MSFC 60,000 lbf FASTRAC rocket engine). Not all of the 60 OSC employees said to be in the OSC X-34 program office are engineers but for the number that are (not stated), they have quite a challenge keeping track of 30 subcontractors.

The ASAP participants identified several possible safety-related issues related to carrying the X-34 to altitude with the L-1011. Overall, little was presented on this topic. The assumption seemed to be made that another group at OSC and/or the FAA would be responsible for L-1011 safety. Since the X-34 is an unmanned vehicle, the greatest risk to humans on the program will likely come from the carry flights and releases. Some specific issues are:

- There is a finite possibility that the X-34 could strike the L-1011 after an inadvertent or planned release in either the initial unpowered drop or subsequent powered flight tests. The reviews did not contain information relating to the analyses and wind tunnel testing that had been done to assure a clean release under all potential flight conditions.

- There was little discussion on the dry weight of the X-34 vehicle, but charts shown indicated that most of a 20% dry weight margin available at program start had been used to date. With the large number of subcontractors involved there are bound to be surprises when the components arrive to be integrated. It would not be unrealistic to suspect that the vehicle will exceed its design weight. If OSC has designed to the maximum lift-off capacity of the L-1011, the only way to get off the ground with the X-34 is to off-load X-34 propellant

because there is no payload of any consequence to reduce. There was no indication that OSC had considered whether propellant sloshing in partially filled X-34 tanks would have detrimental effects on the L-1011 flight characteristics prior to release of the X-34. This could be a potential safety problem.

It would seem prudent for Code Q to assess the risks involved with carrying and launching the X-34 from the L-1011 more completely before the first flight. This may require further meetings with other groups at OSC as well as the FAA. From a programmatic standpoint, it must also be recognized that the L-1011 is a single point failure source. Nothing was said about how the program would recover from a loss or grounding of the single L-1011 that OSC owns.

Another area of possible safety concern is the X-34 flight software. They are using as much "heritage" software (Pegasus, Shuttle, etc.) as possible and performing extensive unit and integrated code testing. The briefing indicated, however, that this is focused on verifying that the code faithfully replicates the functions of the heritage application. There was no mention of the extent to which they are validating that the approach taken by the heritage application is, in fact, appropriate for the X-34. It must be remembered that it was the failure to validate a legacy software application from Ariane 4 that caused the loss of the first Ariane 5.

One of the bigger safety risks in the X-34 vehicle could be the rocket propulsion system. Nothing was said about the feed system although we did see tanks in place in the vehicle on the shop floor. Is OSC responsible for the entire feed system such as the tanks, gas generator, turbopumps, the engine controller, engine valves and other necessary components? Not much was said about the vehicle/engine interface except that MSFC would supply the FASTRAC engine GFE to OSC. With the bolt-on interface implied, how is propulsion system cleanliness maintained? Contamination of the LOX system could be an explosion hazard. What other components will MSFC supply? The engine consists of at least the injector, combustion chamber and nozzle. An ignition system is required because the propellants are not hypergolic. Who is responsible for it? MSFC/Thiokol appear to have done good work on the innovative chamber and nozzle design and fabrication. However, the injector status was not covered thoroughly nor was the extent of the integrated engine (injector, chamber and nozzle) hot fire tests that have been accomplished or are in work. There could be problems with the injector design, and MSFC may be a long way from having a reliable integrated engine design. The thought of engine "fabrication and assembly to print by small and non-traditional vendors" is a little discomforting. Who certifies these non-traditional vendors?

The flight termination system uses the control surfaces to render the vehicle unflyable. As with the X-33, there was no mention of risks involved in terminating a flight with significant amounts of unspent fuel on board. This could be particularly risky for an air launched vehicle that is at a significant altitude when all of its fuel is still available.

One of the objectives of the X-34 program is to obtain experience and information concerning rapid turnaround of RLV type vehicles. Rapid turnarounds involve trade-offs for streamlining the various functions that need to be accomplished between flights. There is the possibility that higher risk will be assumed in order to speed the turnaround. This aspect of the X-34 safety review was not

discussed. It would have been good to see a checklist of operations steps for the initial unpowered and powered flights as well as for the rapid turnarounds. One chart made mention of "integrated health monitoring as a key element in driving the costs down and accomplishing a two week vehicle turnaround." Admittedly, the turnaround job is simplified because there is little weight margin or volumetric capacity in the vehicle for payload, but there are still important steps and safety considerations in determining whether the vehicle is sound for return to flight even as a demonstration vehicle. It also appeared as though NDE was eliminated as too complicated a tool for between-flight verification of the structure, but there was no indication of what would be used in its place. Rocket engine inspection prior to reflight was never even mentioned. Among the safety issues with the engine are propellant loading procedures, engine health parameters to be measured and inspections prior to reflight.

In summary, although the briefings were extensive, they left numerous potential safety-related issues unanswered. This may have been more a result of the focus OSC selected for the presentations rather than any underlying shortcomings. A more extensive examination by Code Q on the topics described above as well as those that may have been identified by other participants is needed to complete a thorough safety assessment of the program.

Implications for Future ASAP Activities

As with the X-33, since the X-34 vehicle is unmanned, there is no need for a large ASAP involvement in the program. However, the Panel should continue to interact with the Code Q team to determine their progress in addressing the issues raised in this memo. The Panel should also continue to monitor the program activities periodically to maintain an understanding of any safety-related decisions. In particular, we should be sure that the L-1011 flight procedures and safety systems are appropriate. We should also examine the range safety plans after WSMR completes their work. WSMR, under subcontract to OSC, has the responsibility for flight safety and flight termination system requirements. Based on the presentations given, their input so far appears to be largely generic but should get more specific as the flight date is approached. In spite of the absence of detail, there is some consolation in the WSMR statement that they have had a perfect safety record for 50 years and that the entire flight path of the X-34 is within WSMR confines.

cc: Fred Gregory